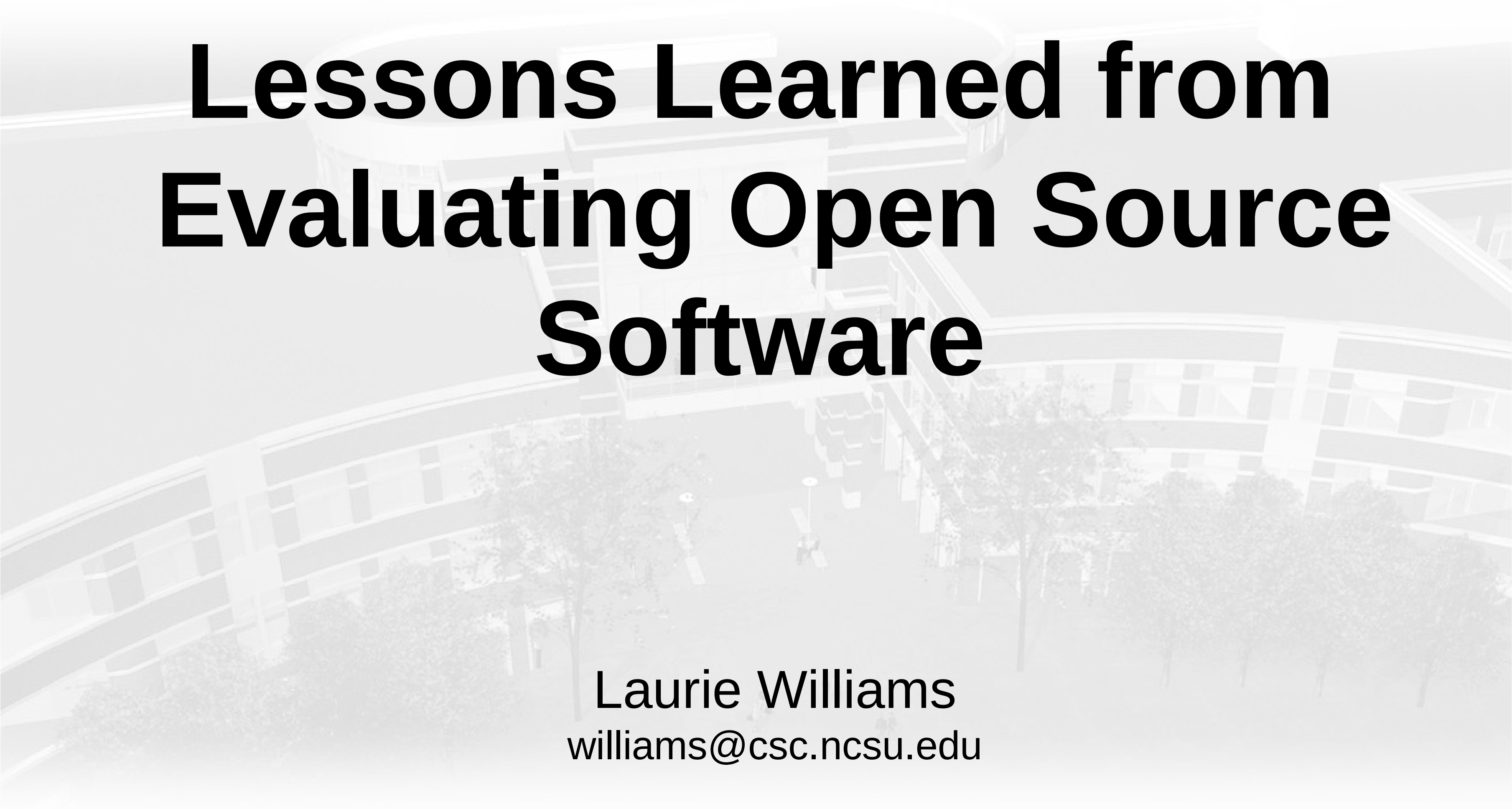
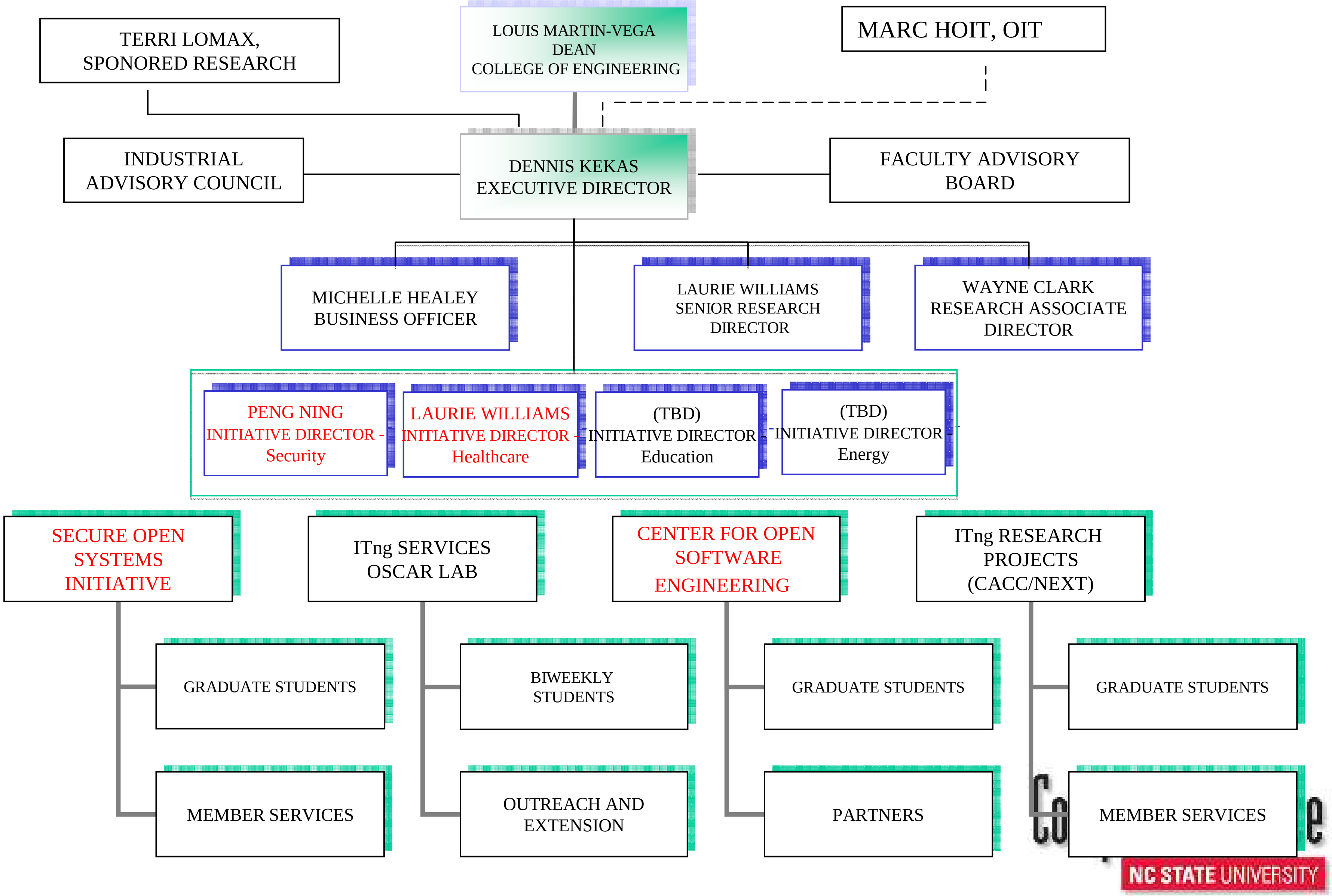


# Lessons Learned from Evaluating Open Source Software

Laurie Williams
williams@csc.ncsu.edu

# INSTITUTE for NEXT GENERATION IT SYSTEMS



TERRI LOMAX,
SPONORED RESEARCH

LOUIS MARTIN-VEGA
DEAN
COLLEGE OF ENGINEERING

MARC HOIT, OIT

INDUSTRIAL
ADVISORY COUNCIL

DENNIS KEKAS
EXECUTIVE DIRECTOR

FACULTY ADVISORY
BOARD

MICHELLE HEALEY
BUSINESS OFFICER

LAURIE WILLIAMS
SENIOR RESEARCH
DIRECTOR

WAYNE CLARK
RESEARCH ASSOCIATE
DIRECTOR

PENG NING
INITIATIVE DIRECTOR -
Security

LAURIE WILLIAMS
INITIATIVE DIRECTOR -
Healthcare

(TBD)
INITIATIVE DIRECTOR -
Education

(TBD)
INITIATIVE DIRECTOR -
Energy

SECURE OPEN
SYSTEMS
INITIATIVE

ITng SERVICES
OSCAR LAB

CENTER FOR OPEN
SOFTWARE
ENGINEERING

ITng RESEARCH
PROJECTS
(CACC/NEXT)

GRADUATE STUDENTS

MEMBER SERVICES

BIWEEKLY
STUDENTS

OUTREACH AND
EXTENSION

GRADUATE STUDENTS

PARTNERS

GRADUATE STUDENTS

MEMBER SERVICES

# Case Study: Linux Kernel

- Red Hat Enterprise Linux 4 Kernel
  - Over 14,000 **source code** files (*.c, *.h, *.s)
  - Over 10,000 **files changed** in the 16 months prior to release
    - Examined **version control change logs**
  - ~200 files found to have a **post-release vulnerability**
    - 2% changed files **vulnerable**, 98% **neutral**
  - ~550 **developers**

Project supported by ARO

# Results: Linus' Law

- Files changed by **many developers** were less likely to have a vulnerability ✗

  *A file was **16 times more likely** to have a vulnerability if it had **9 or more developers** who changed it*
  *(33% vs. 2%)*

- Files changed by **multiple, otherwise-separated clusters of developers** are more likely to be vulnerable than changed by a single cluster ✓

# Results: Unfocused Contribution

- Files changed **many times** were more likely to have a vulnerability ✓

  *Vulnerable files had more commits (p<0.0125) than neutral files.*

- Files with **unfocused contributions** are more likely to have security vulnerabilities ✓

  *Contribution Network centrality was higher (p<0.0125) for files with vulnerabilities*

# Healthcare IT - 1

- Design Flaws:
  - Admin is super power
  - No logging
  - New users given customizable roles
  - Users can “shop around” without a trace
  - … analysis abandoned because we felt it could not be used in the US

Project supported by AHRQ

# Healthcare IT - 2

- Fortify static analysis alerts
  - 440 confirmed true positives (may overlap with below)
  - Cross site scripting, nonexistent access control, dangerous function, path manipulation, error information leak, more…
- Rational AppScan Automated Penetration Testing
  - 130 confirmed true positives (may overlap with above)
  - Cross site scripting, phishing, cross-site forgery, error information leak, SQL injection, more…
- Now working to attack manual black box
- Escapes from CCHIT Security Certification

# Selected Other NCSU Projects

- Is complexity a friend or enemy of security?
- Are specialized vulnerability prediction model desirable (or are fault prediction models sufficient)?
- What is the relationship between disclosed and exploited vulnerabilities?